541-107
CSC/SD-90/6059

MISSION OPERATIONS AND DATA SYSTEMS DIRECTORATE

NASA Communications (Nascom) Access Protection Policy and Guidelines

Revision 3

November 1995

National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

NASA Communications (Nascom) Access Protection Policy and Guidelines

Revision 3

November 1995

Prepared Under Contract NAS5-31500
Task Assignment 46 502

Approved by:

B. Torain, Head Nascom Computer security Official GSFC, Code 541.3	Date

V. Turner, Chief NASA Communications Division GSFC, Code 540	Date

This document supersedes *NASA Communications (Nascom) Access Protection Policy and Guidelines*, 541-107, dated March 1993, and all changes thereto.

Goddard Space Flight Center
Greenbelt, Maryland

Preface

NASA Communications (Nascom) Access Protection Policy and Guidelines provides the policy for limiting unauthorized access to Nascom from a connected Automated Information System (AIS). It outlines the procedures for self-certification of an AIS connected to Nascom**, describes** the audit procedures used to evaluate the AIS security features, and lists the procedures for submission of waivers and circuit requests for new AIS interfaces to Nascom. This document is applicable to all NASA centers, NASA field organizations, NASA program offices, NASA contractors, and foreign countries using Nascom circuits, networks, or facilities.

This document is under configuration control, and the NASA Communications Division is responsible for processing all changes to it. Changes to this document will be issued by document change notice (DCN) or, where applicable, by complete revision. All questions concerning this document should be addressed to:

Chief, NASA Communications Division
Code 540
Goddard Space Flight Center
Greenbelt, Maryland 20771

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Revision 3
iii through viii	Revision 3
1-1 and 1-2	Revision 3
2-1 and 2-2	Revision 3
3-1 through 3-9	Revision 3
4-1 through 4-5	Revision 3
5-1 and 5-2	Revision 3
A-1 through A-13	Revision 3
B-1	Revision 3
C-1 through C-4	Revision 3
AB-1 and AB-2	Revision 3
GL-1 through GL-3	Revision 3

Document History

Document Number	Status/Issue	Publication Date	CCR Number
541-107	Original	May 1990	540.0/183
541-107	Revision 1	March 1992	540.0/277
541-107	Revision 2	March 1993	540.0/345
541-107	Revision 3	November 1995	_________

DCN Control Sheet

DCN Number	Date/Time Group (Teletype Only)	Month/ Year	Section(s) Affected	Initials

Preface

Section 1. Introduction

1.1 General 1-1

1.2 Purpose 1-1

1.3 Scope 1-1

1.4 Background 1-1

1.5 Authority 1-2

1.6 Applicable Documents 1-2

Section 2. Access Control Policy

2.1 Policy Statement 2-1

2.2 Policy Implementation 2-1

2.3 Policy Application 2-1

2.3.1 Inclusions 2-1

2.3.2 Exclusions 2-2

Section 3. User Certification

3.1 Self-Certification of Existing System(s) or of Proposed System Changes 3-1

3.1.1 Responsibilities 3-1

3.1.2 Procedures 3-1

3.2 User-Developed AIS Security Policy 3-1

3.2.1 Desired Goal and Objectives 3-1

3.2.2 AIS Policy 3-1

3.2.3 System Security Architecture 3-2

3.3 Use of Nascom Policy and Guidelines Document and Attached Checklist 3-2

3.4 Evaluation of System Security Features 3-2

3.4.1 General Security 3-2

3.4.2 Security Software 3-3

3.4.3 Physical Security 3-5

3.4.4 Network Security 3-6

3.5 Procedures To Enhance Security 3-8

3.6 Waivers 3-9

3.6.1 Waiver Generation 3-9

3.6.2 Submission of Waivers to Nascom 3-10

3.6.3 Waiver Approvals 3-10

Section 4. Nascom Division-Sponsored Audits

4.1 Authority 4-1

4.2 Notification of Intent To Audit 4-1

4.3 Audit Team Support 4-1

4.3.1 Physical 4-1

4.3.2 Checklist Review 4-1

4.3.3 System Walkthrough 4-2

4.3.4 Other Data Required 4-2

4.4 Audit Team Authority 4-3

4.5 Audit Team Reports 4-3

4.5.1 Update Checklist 4-3

4.5.2 AIS Summary Letter 4-3

4.5.3 Visit Summary Letter 4-3

4.5.4 Coordination of Audit 4-3

4.5.5 Audit Briefings 4-3

4.5.6 Report of Audit Findings 4-3

4.6 AIS Sponsor's Waiver Responsibilities 4-4

4.7 Reaudits 4-4

4.8 Protection of Audit Report and Briefings....................4-4

Section 5. User Requirements for Nascom Service

5.1 Submission for Nascom Service for an AIS....................5-1

5.2 Security Checklist....................5-1

5.3 Block Diagram of System....................5-1

5.4 Physical Layout Security Description....................5-1

5.5 AIS Security Policy....................5-1

5.6 Waiver Requests....................5-2

5.7 Process and Approval....................5-2

List of Figures

4-1 Example of Required System Block Diagram....................4-2

Appendix A. Certification Requirements Checklist

APPENDIX B. Nascom Access Control Policy Waiver Request

Appendix C. MODNET and NOLAN Security Policy

Abbreviations and Acronyms

Glossary

Distribution List

Section 1. Introduction

1.1 General

The NASA Communications (Nascom) Network is a global communications system consisting of many types of communications circuits interfacing with numerous diversified data communications systems and networks. The Nascom Network provides telecommunications in support of operational National Aeronautics and Space Administration (NASA) projects and mission activities, including manned and unmanned space missions.

To protect this valuable resource, all Automated Information Systems (AISs) that use Nascom must be designed and operated so that sensitive space communications operations are not interrupted, distorted, or captured by unauthorized parties. **An AIS refers to any equipment or interconnected system or subsystem(s) of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and information. This includes mainframe computers, minicomputers, microcomputers, workstations, word processors, automated office support systems, communications systems, networks and their interconnecting hardware, and test equipment.**

1.2 Purpose

This document specifies the policy for limiting unauthorized access to Nascom from a connected AIS and prescribes the procedures for self-certification of an AIS connected to Nascom. It describes the audit procedures used to evaluate the security features of a Nascom-connected AIS, outlines the procedures for submission of waivers for an AIS not meeting the full protection criteria, and lists the information required for submission of circuit requests for new AISs.

This document does not replace any security directives, documents, or policies created by the local NASA center or NASA Headquarters, but is an additional requirement for any AIS that has an interface to Nascom. Should this document conflict or require different security measures than any other user institution requirements, the strongest, most stringent security requirement should be implemented.

1.3 Scope

This document is applicable to all NASA centers, NASA field organizations, NASA program offices, NASA contractors, and foreign countries using Nascom circuits, networks, and facilities.

1.4 Background

Communication and computer networks are recognized to be vulnerable to unauthorized access and can be subject to interruption or damage unless system design precautions and security-oriented operational control procedures are employed. NASA Headquarters has directed that the design, implementation, and operation of any AIS using Nascom's worldwide network be evaluated to ensure that each system connected to Nascom is not vulnerable to unauthorized access and will not allow disrupting forces in any way to adversely impact Nascom operations.

1.5 Authority

NASA Handbook (NHB) **2410.9A** (Chapter 4) provides guidance for determining automated information categories and sensitivity or criticality levels for that information. Once the category and sensitivity or criticality levels have been determined, the handbook establishes a protective-measure guideline that is appropriate when this information is processed by an AIS or transmitted over a communications network. Using this handbook and the referenced documents (Section 1.6), Nascom has created this policy and guideline document to provide a more specific set of protective measures and criteria for AISs that interface with Nascom.

1.6 Applicable Documents

a. National Telecommunication and Information Systems Security Policy No. 200, "National Policy on Access Control Protection"

b. Public Law 100-235, "The Computer Security Act of 1987," January 8, 1988

c. NMI **2410.7C**, "Assuring the Security and Integrity of NASA Automated Information Resources," **April 08, 1993**

d. NASA Headquarters Letter, "Nascom Access Control Policy," August 4, 1988

e. NMI 2530.00, "Telecommunications Systems-Terrestrial and Spaceflight—Security Policy and Implementation Guidelines," January 31, 1990

f. NASA Automated Information Security Handbook NHB **2410.9A, June 1993**

g. NMI 2520.1D, "Communications System Management," November 18, 1991

h. 541-225, "MODNET and NOLAN User’s Guide," May 1995.

Section 2. Access Control Policy

2.1 Policy Statement

The Nascom Access Control Policy, hereafter referred to as the Policy, is intended to preclude unauthorized access and potential damage to the Nascom operational system and user AISs that use Nascom data services.

The user institutions shall ensure that access to Nascom data lines is restricted to interfaces controlled by the Nascom Division in the GSFC Mission Operations and Data Systems Directorate (MO&DSD).

The user institutions shall ensure that access to Nascom data lines is restricted to preclude unauthorized access.

2.2 Policy Implementation

The user institutions shall examine each AIS that interfaces with Nascom and, using the guidance contained herein, shall perform a user self-certification for each appropriate AIS.

If the user institution determines that the subject AIS cannot meet the specified security criteria, an appropriate waiver must be submitted to the Nascom Division, GSFC, as described in Section **3.6** of this document.

The Nascom Division will evaluate the waiver and will either provide approval or recommend an alternate approach to resolving the discrepancy.

As authorized by the Policy Letter (Authority 1.5.c), the Chief of the Nascom Division will direct audits to be performed at each user installation, as required. The Nascom Security Audit Team, hereafter referred to as the Audit Team, will be allowed access to the self-certification data, analyses, waiver requests, and any security-related reports.

NOTE

> Testing, simulations, or operational support will NOT be permitted on any new circuit without a **completed security certification checklist, a modification to a previously submitted checklist if it is less than two years old, and a Code 540 approved waiver request, if applicable.**

2.3 Policy Application

2.3.1 Inclusions

This policy applies to any AIS that has Nascom-supplied data circuits that pass to or through GSFC and interface through one of the following systems:

- Message Switching System (MSS)
- Data Distribution and Command System (DDCS)

- Message and Packet Switching System
- GSFC MO&DSD Operational Development Network (MODNET) and Nascom Operational Local Area Network (NOLAN)
- Multiplexer/Demultiplexer (MDM) Data System
- Digital Matrix Switch (DMS)
- **Earth Observing System Data and Information System (EOSDIS) Backbone Network (EBnet)**

NOTE

> The policy also applies to any AIS that is networked to an AIS that meets these conditions.

2.3.2 Exclusions

The policy does not apply to

- Voice, teletype (TTY), or video services
- Simplex (receive only) services with no acknowledgments
- Department of Defense (DOD) approved services
- Point-to-point data services that do not interface through GSFC

Section 3. User Certification

3.1 Self-Certification of Existing System(s) or of Proposed System Changes

3.1.1 Responsibilities

Each user institution or sponsor of an AIS is responsible for the hardware and software configuration and the required level of security protection. Each user is also responsible for certifying that the respective system, as designed and operated, will not allow unauthorized users to penetrate the connecting Nascom circuitry. Unauthorized users include both those not authorized to access the AIS and legitimate users of the AIS not authorized to access the specific piece of information or process being protected. Measures used to implement this protection can consist of hardware and software or operational procedures, or a combination thereof.

3.1.2 Procedures

Each user should examine the Nascom circuit terminations at the respective facility and determine which AISs using Nascom must be certified to meet the security features described in Section **3.4** of this document. If any system(s) must be certified, the user should use the procedures described in the following section to assist in the evaluation and certification.

3.2 User-Developed AIS Security Policy

3.2.1 Desired Goal and Objectives

The goal of the Nascom AIS security program is to provide cost-effective protection that ensures the integrity, availability, and confidentiality of Nascom automated information resources. The objectives are to

- Protect against deliberate or accidental corruption of Nascom automated information
- Protect against deliberate or accidental actions that cause Nascom automated resources to be unavailable to users when needed
- Ensure that there is no deliberate or accidental disclosure of NASA sensitive automated information

3.2.2 AIS Policy

The user institution security policy for an AIS resource that connects to Nascom shall provide a level of integrity consistent with management's determination of an acceptable level of risk, sufficient to ensure that the Nascom AIS resources operate effectively and accurately, and protects data from unauthorized access, alteration, destruction, disclosure, or abuse. The Nascom AIS resources must maintain continuous support of NASA missions and programs, while simultaneously incorporating operational and functional controls sufficient to provide assurance of integrity, availability, and confidentiality. To accomplish this, Nascom AIS resources must be provided with appropriate technical, personnel, administrative, and environmental safeguards. The policy must also address the security requirements for expansion of the AIS when adding new components or connecting new interfaces such as local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), or international networks, such as the Internet.

3.2.3 System Security Architecture

To evaluate an AIS constructed from components built independently, the AIS security architecture and design shall completely and unambiguously define the security functions of components, as well as the interfaces between or among components. The AIS sponsor shall develop a high-level block diagram that depicts the complete hardware configuration of the system and includes all interfaces with external telecommunications and computer systems. This diagram shall show all repeaters, servers, bridges, routers, **firewalls**, and gateway components and describe how these interface devices affect the security of the AIS (e.g., act as a physical switch, require passwords, pass only selected addresses, pass selective protocols).

A user institution or sponsor of an AIS is responsible for maintaining current hardware inventory and configuration drawings. At the very least, these drawings should be reviewed and updated every six months.

3.3 Use of Nascom Policy and Guidelines Document and Attached Checklist

This Nascom policy and guidelines document summarizes the certification process and includes blank forms and examples of system block diagrams. This document is meant to provide guidelines and does not stipulate specific security requirements or design parameters to be followed. The audit checklist (Appendix A) provides insight into the security areas that should be evaluated in the self-certification process; this checklist will be used by the Nascom Audit Team during onsite audits.

3.4 Evaluation of System Security Features

3.4.1 General Security

There are many areas of an AIS that are evaluated for possible vulnerabilities. These are covered under Security Software, Physical Security, and Network Security in the subsequent subsections. There are some additional items that should be noted:

A security policy should be maintained for all AISs with Nascom connectivity. The policy should address the AISs and it should be enforced.

Clear text passwords should not be stored on the system, nor used with external networks.

The number of privileged accounts or super users should be restricted to a small set of users (ideally one to three maximum).

A risk analysis should be performed at least every 3 years.

Annual security training should be provided for all personnel using a Nascom connected AIS.

All new software should be checked for viruses before loading the software onto the system.

Systems should refrain from providing banner type information about the system, or permitting HELP information until after a user has successfully logged into the system, and has been authenticated.

Remote users should be restricted to certain partitioned directories, local files, services and commands. The use of proxy servers is another way to protect commonly utilized services, such as File Transfer Protocol (FTP).

All areas of the network should be under configuration management. This includes bridges, routers, gateways, and their configuration and routing tables; interfaces to LANs, WANs, and MANs; and security and system software.

Contingency plans and software backups should be maintained and tested.

3.4.2 Security Software

The majority of computer systems (AISs) interfacing with Nascom have vendor-supplied or third-party software packages to provide security enhancement(s). **Both system and security upgrades should be maintained to ensure the lastest defenses against known vulnerabilities.**

While each computer manufacturer addresses the security problems and solutions uniquely, there are several common parameters that the self-certification process should address: user Ids, passwords, file, command, and service access, security monitoring and auditing, physical security, and network security.

3.4.2.1 User Ids and Passwords

The default accounts and passwords placed by the manufacturer during installation should be checked to ensure that they have been changed, removed, or disabled.

System or executive account(s) used to make modifications to the system, add and update system software, **and** add or delete users to the system should have secondary passwords, if possible. (These accounts should be audited for every access.) **All** passwords should be unique, **difficult to guess, and include at least one alphanumeric or special character. (Use of the beginning letters of a phrase with an alphanumeric or special character inserted could be used.)**

One-time or encrypted passwords are preferable for those AISs with remote access to their networking equipment, hosts or file servers through modems, terminal servers, and TELNET commands.

Dial-in modems, including dial-back modems, should be evaluated carefully before implementation.

Ensure that user accounts have acceptable passwords or pass phrases that are changed on a regular basis. User passwords should be at least 6 (preferably 8) characters in length, **difficult to guess, and include at least one alphanumeric or special character. The passwords should expire within 180 days (90 days preferred) for hosts on AISs with auditing capabilities, and within 90 days (30**

days preferred) for hosts on AISs with no auditing capabilities. Ensure that the operating system will disable the account 5 to 10 days after the password life has expired.

Firewalls, routers, bridges, gateways, and other configurable devices should also adhere to these password rules.

If terminal servers are used in the system, enable terminal server passwords, if possible, and enable a password on every port that has a modem associated with it.

User authorization records should be periodically inventoried and all inactive users or users with expired passwords removed. For large systems with rapid turnover or reassignment of computer personnel, formal procedures for administering and controlling the users should be established to keep the authorization records current.

3.4.2.2 Files, Commands, and Service Access

Unauthorized access to application files and programs may be reduced by controlling users with captive menus, **or the file protection system which is used by the operating systems to grant file access and privileges. Certain software, such as the password guessing CRACK program, should be restricted to the security personnel.**

3.4.2.3 Security Monitoring and Auditing

Visual as well as audible security alarms inform the security manager when a probable access by an unauthorized user has been attempted. Ensure that the critical alarms are set and audit features activated.

The AIS should create, maintain, and protect from modification or unauthorized access or destruction, an audit trail of accesses to the objects it protects. Successful, as well as failed attempts, should be recorded. The audit data should be protected by the AIS so that read access is limited to those individuals who are authorized for accessing audit data. The AIS should provide the capability to record the following types of events:

a. **Use of identification and authentication mechanisms (e.g., login, logoff)**

b. **Introduction of objects into a user's address space (e.g., file open, program initiation)**

c. **Deletion of objects**

d. **Actions taken by computer operators and system administrators or system security officiers and other security relevant events**

e. **Accesses to sensitive files**

f. **Suspends, and accidental or deliberate disconnects.**

It is recommended that, as a minimum, system auditing include break-in attempts, accesses from detached processes, modifications to user authorization files, and remote accesses.

For each recorded event, the audit record should identify the following:

- a. **Date and time of event**
- b. **User**
- c. **Type of event**
- d. **Success or failure of event**
- e. **For identification or authentication events, the origin of request**
- f. **For introduction or deletion of objects, the name of the object.**

The audit records should be reviewed bi-weekly, at the minimum.

The system administrator should be able to selectively audit the actions of any one or more users based on individual identity. There should be an automatic audit log review function to examine all logs. There should be reporting functions that readily and clearly provide user profile, access rules, and reports on audit log data. Report writer or audit tools should include the following abilities to select for reporting:

- a. **Security audit log records for review**
- b. **System security parameter settings**
- c. **User attributes**
- d. **File and directory protection levels**
- e. **Security system configuration, password, and data protection exposures.**

3.4.3 Physical Security

The computer equipment should be located in a controlled facility that provides for limited access. **The AIS and relevant equipment (i.e., hosts, file servers, network wiring, hubs, routers, gateways**, **firewalls, etc.) should be secured in rooms** with access devices that log and control each individual's entrance to the room. **These rooms should post a current access list of personnel authorized for access to the area. There should be a sign in and sign out log for visitors, and escorts should be provided, when necessary.**

Unused equipment should be properly and securely stored to prevent unauthorized connection to the AIS. Inventories of both the hardware and software configurations should be maintained and kept current.

A system console offers a direct access into the system. The console should be located in a secure area. Computer centers with multiple AISs may want to locate all system consoles separate from the main computer area. Access to the system console should be restricted to the computer operations staff.

Unattended terminals, especially those logged into a privileged account, are a dangerous security breach and can allow intruders free access to the system with minimal risk of

detection. The user community should be encouraged to log off from the system when leaving for a break. Systems could be provided with one of many watchdog programs that will automatically log off a user after a preset number of minutes of inactivity (preferably 5 to 15 minutes). If available, this feature should be activated, especially for the AIS terminals that are located away from the main equipment room or operations area.

Terminal servers; network interface equipment such as bridges, routers**, firewalls**, and gateways; and network test equipment should be located in a controlled facility that provides for limited access. The network test equipment, such as protocol analyzers, should be restricted to authorized personnel and accountability for their use maintained.

Terminals and workstations should be secured, or located in secure areas. If a user must remain logged on, they should use password-required screen savers. This is in addition to the required user ID and password for initial signon to the terminal or workstation. Operations terminals in controlled areas or those manned 24 hours per day do not need this feature.

3.4.4 Network Security

Because the goal for Nascom AIS resources is to ensure the integrity, availability, and confidentiality of sensitive automated information, any network connection should also have these same **goals.**

When a user AIS connected to Nascom is also connected to another network, or when a user network connects to Nascom, access to all components of this new network should meet the requirements and goals of this document. While each Nascom user will address these goals uniquely, the self-certification process should address the following common areas:

The system administrator for an AIS that interfaces with LANs, WANS, or MANs should examine the security features of the interconnecting network(s). If a connecting network has minimal security **or** if the interface allows free access between the systems, the AIS security protection could be compromised. The administrator should consider disabling the interface, upgrading the connecting network to the proper AIS level of security, or providing a secure interface between the two systems.

Physical access to the network, including wiring, should be restricted to the greatest extent practical. Local wiring, including LAN cabling, should have unique identifying cable tags and be periodically checked for unauthorized taps.

Use of network security software tools, such as CRACK, SATAN, etc., should be restricted to authorized users only. This should be reiterated in the security policy.

Systems with remote-access capability should be carefully controlled to ensure that remote users have minimum access to local files and, if possible, that remote entries are limited to a specific set of menu-driven actions.

In the Client/Server architecture, the LAN operating system will provide the basic system security and audit features. If the operating system does not provide adequate security features, add-on software should be included to satisfy security and audit requirements.

Dial-in interfaces provide widespread exposure of an AIS or network to would-be penetrators. User institutions should minimize this exposure. Break-before-make-type dial-back modems are effective for preventing unauthorized access. Also, modems should have enable passwords, in addition to log-on passwords, for the system. Telephone numbers for dial-in interfaces should be changed periodically**, especially after personnel or temporary hires have terminated.**

If the Nascom-connected AIS does not provide adequate security protection or restrictions between the Nascom Network and other connected networks, each AIS connected on these other networks must comply with the security provisions outlined in this document. Additionally, these AISs connected to other networks may also be audited by the Nascom Audit Team.

3.4.4.1 Bridges, Routers, Gateways, and Firewalls

The interface between an AIS and a second network can consist of a bridge, router, gateway, firewall, or channel-attached connection, depending on the protocols selected and the distance between the networks. These components will vary in their ability to support the overall security objectives. They should be evaluated to ensure that they meet the proposed security architecture of the Nascom connected AIS.

As mentioned before, the rules and guidelines for workstation passwords are applicable to bridges, routers, firewalls, and gateways. Whenever possible one-time passwords, such as smart cards, or tokens, such as Kerberos, should be implemented. Source routing should be disabled on all routers. TELNET to routers should be disabled and all maintenance and software changes should be initiated from a local console. All configuration and software changes should be maintained under configuration management.

Using the same password for more than one router in the same network or network(s) compromises the other routers when the password on one of the routers is cracked.

The configuration of a router or firewall should reflect the security policy of the AIS(s). If the policy reflects "everything not denied is permitted," then the router or firewall will not protect the AIS(s) as much as a policy which reflects "everything not permitted is denied."

It should be noted that with routers the general rule is that everything not denied is permitted, and with a firewall, everything not permitted is denied.

Routers themselves now offer a vulnerable point in a network. Authentication and restricted access should be maintained. Internal routers should restrict sending their routing tables to external routers. Router's access control lists should be carefully constructed to reflect the security policy, and the documentation of these lists securely maintained. TELNET to a router should not be enabled. The use of TELNET to a router may make a system administrator's job easier, but this too opens a vulnerability.

Routers and firewalls should not be viewed as the total solution for security. Routers and network level firewalls look at headers, acting as packet filters. Routers and firewalls should be configured such that no internal addresses are allowed to pass from the outside to the network.

NOTE

Use routers and firewalls to restrict access to your network, but do not rely on them completely, and certainly not exclusively.

3.4.4.2 Network Monitoring and Auditing

The network manager should make periodic checks of the network, particularly at the Nascom interface, to verify proper operation and to detect any unaccountable changes in operations. One or more persons should be assigned to conduct these checks at frequent, random times. A terminal should be designated to monitor network activity, including the Nascom interface.

Test equipment **and network monitoring software** can be used as a tool to penetrate a network and to perform unauthorized actions. Therefore, test equipment should be physically controlled and records should be maintained to provide an audit trail of equipment use. Equipment used to continuously monitor a network or interface, such as data scopes or protocol analyzers, should be located in a secured area or under the continuous supervision of responsible persons. **Network monitoring software, such as Openview, and sniffer-type programs, such as Etherpeak, should be restricted to authorized personnel only. An audit trail should be provided on any attempts at its use.**

3.4.4.3 MODNET and NOLAN Connectivity

There are specific requirements that must be met for those AISs with connections to the MODNET-NOLAN operational Nascom LAN. Appendix C details the MODNET-NOLAN Security Policy with which users must comply.

3.5 Procedures To Enhance Security

In addition to the security features that are evaluated by the Audit Team, users may implement some of the following procedures to enhance the security of their AIS and network:

- Identify opportunities to enhance security in the development and maintenance life cycle of user software.
- Develop local coding standards and procedures, beyond those supplied by software vendors, and require software development personnel to adhere to them.
- Ensure that all modifications to and new releases of the operating system are installed in a controlled manner.
- Establish a product assurance or quality control group to verify that standards are followed and that all software (new or upgrades) is necessary and valid.
- Establish an independent system or acceptance test team.
- Run a standard regression and performance test for each software delivery, and compare results with prior tests.
- Establish separate configuration management (CM) and quality assurance (QA) organizations or at least ensure that CM, QA, and software development report to different managers.
- Maintain a master copy of all delivered software in CM that is not accessible by software personnel.

- Identify and implement additional changes to the operating system and applications software that, if made, would provide additional protection to Nascom circuits.
- Search for security features or provisions, beyond those covered in the Nascom Access Certification Checklist, and correct any deficiencies or implement enhancements to improve security.
- Search for and identify backdoors, trapdoors, Trojan horses, or similar paths to penetrate your AIS, network, or Nascom, and take steps to nullify them.
- **Subscribe to security newsgroups or other publications to keep current on the latest problems, and fixes.**

3.6 Waivers

3.6.1 Waiver Generation

Waiver generation is the user organization's responsibility. Waivers should be submitted for any recognized vulnerability as a result of a periodic risk analysis, penetration analysis, self-audit processes, or official Nascom audit if the vulnerability cannot or will not be corrected within 60 days of its identification.

3.6.1.1 Waiver Format

If the self-certification process uncovers a recognizable system vulnerability that will not be corrected within 2 months, a waiver must be prepared and submitted to the Nascom Division. The waiver request should describe the deficiency, proposed solution, impact of the proposed solution on current activities, and expected duration of the waiver.

Appendix B of this document contains a suggested format for the essential elements of a waiver request. The waiver form lists the primary subjects to be addressed (i.e., system name, deficiency description, requested duration of the waiver, and justification). The description of the deficiency and the wording of the waiver request must provide the essential information necessary to allow for an understanding and an evaluation of the deficiency by Nascom Division personnel. The AIS name and deficiency description must be sufficiently unique to allow for identity-tracking of the submission. Each waiver request should be on a separate form to assist in the control and processing of requests.

A completed checklist on the AIS should be submitted with the waiver if one has not been done by the NASA Audit Team since the last major system change.

3.6.1.2 Waiver Duration

Once a deficiency is recognized, the AIS sponsor should estimate the time and cost to develop a solution. An estimate of the length of time for which the waiver is needed expedites the decision-making process for waiver approval and, in addition, establishes a target date for implementation of the fix.

For the convenience of reference, waivers have been divided into three classes:

- Temporary (**4** to 6 months)

- Long-term (7 to 36 months)
- Permanent (more than 36 months)

3.6.2 Submission of Waivers to Nascom

NASA NMI 2530 (Authority 1.5.b), among other directives, designated the Nascom Division of GSFC as the organization responsible for controlling the types of interfaces allowed to Nascom. All requests for waivers of security deficiencies found in an AIS interfacing with Nascom should be forwarded to

Chief, NASA Communications Division
Code 540
Goddard Space Flight Center
Greenbelt, Maryland 20771

3.6.3 Waiver Approvals

The Nascom Division of GSFC will designate a team of communications engineers and AIS specialists to evaluate all waiver submissions. If the submission lacks adequate information for a comprehensive evaluation, this team will contact the submitting sponsor for additional input, as necessary. This approval sequence should be completed within 60 days, unless the waiver is of a magnitude such that NASA Headquarters must be consulted.

Section 4. Nascom Division-Sponsored Audits

4.1 Authority

NASA Headquarters (see Authority 1.5.c) directs the Chief of the Nascom Division, Code 540, GSFC, to perform audits at user installations, as required.

4.2 Notification of Intent To Audit

Although the above directive authorizes unannounced audits, the current practice is to coordinate the visit by telephone or written correspondence with the Center Designated Security Officer (CDSO). The dates for the audit will be chosen so as not to interfere with active space flight mission periods.

The Nascom Audit Team will supply a blank soft-copy of the latest version of the checklist, in a Microsoft Word format, a hard-copy version of the same checklist, and a copy of the Nascom Access Protection Policy Guidelines, if needed.

The Nascom Audit Team will have security clearances for material up to SECRET level. The team's clearances will be forwarded to the Center Security Office before the Audit Team arrives on site.

4.3 Audit Team Support

4.3.1 Physical

The CDSO should attempt to provide the Audit Team with temporary office space for two or three people. Arrangements should be made with the Center Security Office for visitor badges to be issued to the Audit Team for the expected duration of the audit. To expedite the entire process, these badges should be available when these personnel arrive on site. A telephone should also be made available for the Audit Team's use. An IBM-compatible personal computer (PC) loaded with Microsoft Word would also be useful.

4.3.2 Checklist Review

The CDSO should ensure that a completed checklist**, preferably a soft-copy version in Microsoft Word format**, is available for each AIS that will be audited during the visit. The CDSO, or a designated representative, should assist the Audit Team by arranging for interviews with the system managers or system administrators and any other personnel who helped complete the questions on the checklist. Because the questions can be misinterpreted or the answers incomplete, a face-to-face meeting is usually essential to clarify any lack of understanding. At many locations, responsibility for various segments of the system (e.g., system hardware, software, security, audit reports) is assigned to different people; therefore, specialists in each segment may be required for these interviews.

In addition to this checklist completed by site personnel prior to the visit, the Audit team will complete a second checklist. The second checklist will contain follow-up questions to ones on the first checklist, and observations made by the Audit Team during the walk-through and interview process.

4.3.3 System Walkthrough

A knowledgeable system manager or system administrator should be prepared to conduct a system walkthrough with the Audit Team and be able to provide a demonstration of any of the system's security features requested by the Audit Team.

4.3.4 Other Data Required

The following additional data should be supplied to the Audit Team:

- A copy of the locally developed security policy and plan for the system
- A system-level block diagram showing the major system components and the external interfaces (Figure 4-1 illustrates the level of detail needed for this block diagram.)
- A copy of the operational procedures, especially if these procedures are part of the system security

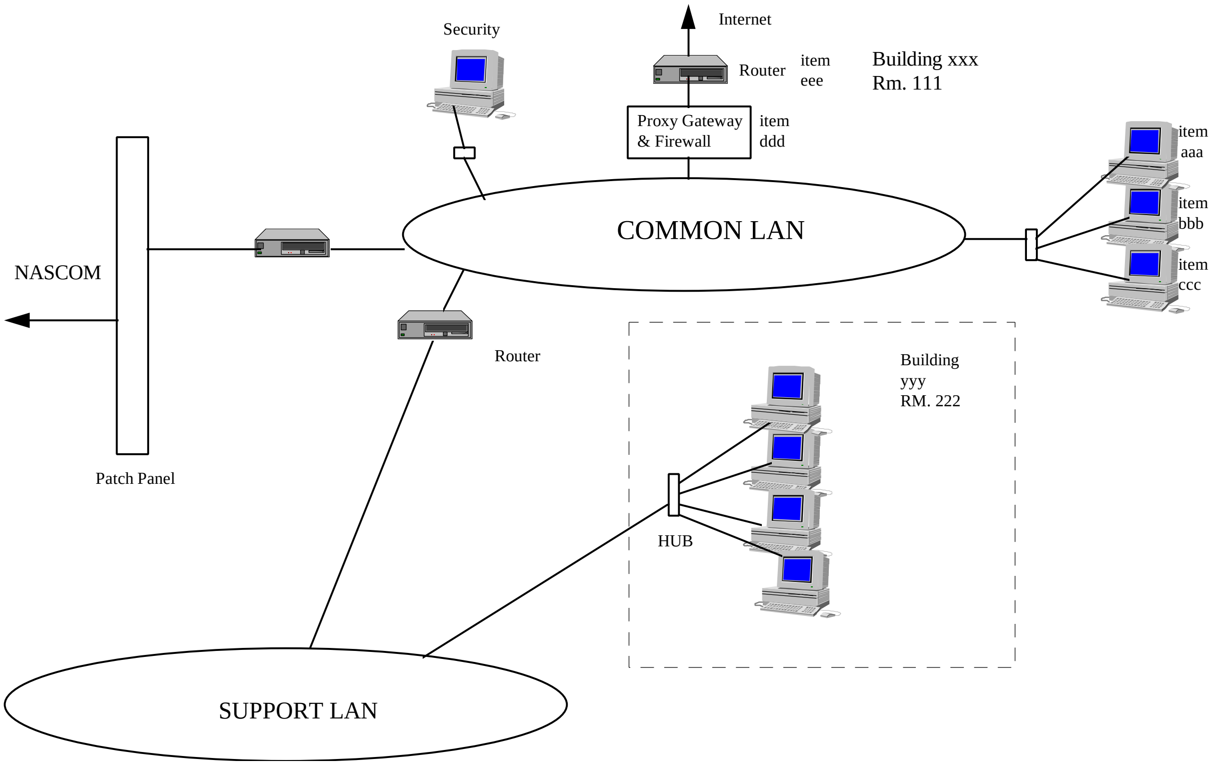

Figure 4-1. Example of Required System Block Diagram

4.4 Audit Team Authority

It should be made clear to the individuals assisting in the walkthrough, and system demonstrations if necessary, that the Audit Team is authorized to view any and all security features of the system being audited. This includes management controls, access controls, audit trails, password management, monitoring capabilities for AIS access, related operational procedures, listings of all authorized users, and interface descriptions.

The Audit Team will not attempt to gain access or log onto the system. The approach to be used by the Audit Team will be to identify system weaknesses or vulnerabilities by observation and by personnel interviews.

4.5 Audit Team Reports

4.5.1 Update Checklist

If time is available, the Audit Team will prepare or update each checklist being reviewed based on the local interviews and the system performance demonstrations, and they will coordinate the contents with the appropriate personnel. **This includes the second checklist, completed by the Audit Team during the onsite visit and interviews**.

4.5.2 AIS Summary Letter

The Audit Team will prepare a summary letter that describes the significant findings for each system audited. The summary letter will identify any system vulnerabilities found and recommend any waivers that appear appropriate. The summary letter may also include recommendations on corrective actions and waiver approval.

4.5.3 Visit Summary Letter

If several systems are audited, the Audit Team may prepare an overall summary letter that summarizes all findings and highlights unique findings on any individual system.

4.5.4 Coordination of Audit

If time is available, copies of the checklist**s** and summary letter(s) will be coordinated with the CDSO prior to the exit of the Audit Team. This is an attempt to ensure that all parties are in agreement with the findings or, at a minimum, to identify and clarify any points of disagreement.

4.5.5 Audit Briefings

The CDSO may request that the Audit Team give an entrance and exit briefing on the intent or findings of the audit. The exit briefing would be essentially the verbal presentation of the summary letter(s).

4.5.6 Report of Audit Findings

These reports are the results of the audit and are forwarded to the Chief of the Nascom Division for review and approval. On approval, segments of the report or the complete report file is forwarded to NASA Headquarters to document the audit findings.

4.6 AIS Sponsor's Waiver Responsibilities

If the Audit Team uncovers a system vulnerability not previously documented, it will be the AIS sponsor's responsibility to submit a waiver request on the identified deficiency. The Audit Team will note the deficiency in its report(s) to the Chief of the Nascom Division and to NASA Headquarters. However, this does not relieve the sponsor of the obligation to either correct the deficiency or request a waiver until the deficiency is corrected.

4.7 Reaudits

The Audit Teams are charged with a yearly examination of the AISs served by Nascom. After the first year, the reaudits will concentrate on the following:

- Systems with existing waivers or waivers discovered in previous audits
- Major hardware or software changes to previously examined AISs
- All systems at least every 3 years if neither of the above-listed situations apply

4.8 Protection of Audit Report and Briefings

Because the Audit Team's reports and briefings may contain information useful to a person seeking to penetrate the system, all completed checklists, reports, and briefing materials must be handled as SENSITIVE DATA—NOT FOR PUBLIC DISCLOSURE and receive limited distribution to those with a need to know.

Section 5. User Requirements for Nascom Service

5.1 Submission for Nascom Service for an AIS

The security policy promulgated in NASA NMI 2530.00 (Authority 1.5.b) specifies that all programs and telecommunications systems have security and protection requirements established at the time of program definition. In accordance with this policy, all requests for Nascom Communications services that interface with an AIS that meets the Nascom Access Control Policy criteria listed in Section 2 of this document must include an access protection analysis as described below.

The Project or user will make a request to the Communications Engineer (CE) for a new Nascom circuit, or a modifcation to an existing circuit. The CE will determine if a new security checklist or a modification to the previous checklist is needed, based on the criteria in Section 2 of this document. To be included with the checklist are the following items: a block diagram of the system, a description of the physical security provided for the system, a copy of the AIS Security Policy and Security Plan, and any waiver request that may be needed.

5.2 Security Checklist

If a new checklist is needed, the Project or user making the circuit request shall provide a copy of a completed (i.e., filled in) checklist. If a modification to a previously submitted checklist is permitted, the Project or user may submit, in writing, the changes. Modifications to a previously submitted checklist are permitted if the existing checklist is less than two years old. A blank copy of the checklist is provided as Appendix A to this document.

5.3 Block Diagram of System

When providing the checklist or modifications to an exisiting checklist, the Project or user will provide **an up-to-date** block diagram of the AIS showing all outside interfaces, including the Nascom interfaces.. Figure 4-1 provides an example of the level of detail needed for this diagram.

5.4 Physical Layout Security Description

The **Project or user** shall provide a description of the intended location**(s)** of the **AIS and relevant equipment (i.e., hosts, file servers, network wiring, hubs, routers, gateways, firewalls, etc.)** and the physical security planned for the location**(s)** (e.g., keylocks, passcards). A description of the physical security planned for any terminals to be located in an area separate from the main computer facilities shall also be provided.

5.5 AIS Security Policy

The **Project or user** shall include an AIS security policy **and security** plan that describes the major elements provided to control access to the system. Section 3.2 of this document describes some of the security elements that should be addressed. For instance, such details as the type of vendor software security system to be employed [e.g., remote-access control facility (RACF), Sentry, ACF2, Top Secret] should be specified.

5.6 Waiver Requests

If, during the generation of the **security checklist** and supporting documentation, the **Project or user** determines that the security approach cannot meet the access control policy criteria, a waiver request shall be submitted for the recognized vulnerability. The procedures for waiver preparation are described in Section **3.6** of this document.

5.7 Process and Approval

The CE will generate the Communication Service Request (CSR), and forward a copy of the CSR, along with the above-mentioned security information which is provided by the Project or user, to GSFC, NASA Communications Division, Mission Planning Section, Code 542.1. Incomplete submissions will delay the approval cycle and implementation of the required service.

Appendix A. Certification Requirements Checklist

A blank copy of the Certification Requirements Checklist is provided in this appendix.

NASCOM ACCESS CONTROL POLICY

Certification Requirements Checklist

____
(Date Completed)

NOTE: The term "Automated Information System (AIS)" refers to the following:

"Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and information. This includes mainframe computers, minicomputers, microcomputers, workstations, word processors, automated office support systems, communications systems, networks and their interconnecting hardware, and test equipment."

A. CONFIGURATION

1. Name the Automated Information System (AIS) (computer system) addressed in this questionnaire.

2. Describe the operational mission functions that this system performs.

** 3. Provide legible block diagram(s) that identify primary terminals, PC's, bridges, routers, gateways and external interfaces to the system, and to other networks. These diagram(s)should indicate the physical location by building and room number of each major component of the system including terminals. Any external interfaces to include access by bus, channel, front-end ports, terminal servers, bridges, and routers should be identified.

Attach copy.

4. Identify which networks or systems (open and closed), this AIS connected to (i.e., ILAN, Internet, center LANs, etc.) :

Internet or NSI? yes _____ no _____

MODNET and NOLAN (Open Segment)? yes _____ no _____

MODNET and NOLAN (Closed Segment)? yes _____ no _____

EBnet? yes _____ no _____

Multiplexor/Demultiplexor (MDM)? yes _____ no _____

Nascom 2000 Data Transmission? yes _____ no _____

DDCS (Data Dist. Comm. System)? yes _____ no _____

Local LANs (Operational only)? yes _____ no _____

Local LANs (Site-wide)? yes _____ no _____

PSCNI? yes _____ no _____

Other? _______________ yes _____ no _____

5. Identify any of the following items which is connected to the AIS or one of its connecting networks:

PCs? yes _____ no _____

MACs? yes _____ no _____

Servers? yes _____ no _____

UNIX Workstations? yes _____ no _____

Remote Access? yes _____ no _____

Other Terminals? _______________ yes _____ no _____

6. Describe the security methods (both hardware and software) that are in place to protect this AIS.

7. Is client/server architecture used in this AIS?

yes _____ no _____

8. On the block diagram(s) provided for question 3, identify all Nascom interfaces to the AIS. Also provide the specifics on the hardware used to accomplish the actual interface(s).

9. Is the software development system for this AIS capable of

transmitting data directly or indirectly over Nascom circuits, or to Nascom systems?

yes _____ no _____

If yes, provide block diagram(s) identifying all components of the software development configuration.

Attach copy.

**10. Are there physical access controls in place for all components of this AIS?

yes _____ no _____

**11. Identify by title or position the individuals responsible for security of the AIS, including the Network Administrators for each local Lan.

Individual	Title	Organization	Phone #

**12. Is the security policy specific or generic for this AIS?

specific _____ generic ______ none _____

Please provide a copy.

13. Are firewalls used on LANs and WANs?

LANs		**WANs**	
yes _____	**no _____**	**yes _____**	**no _____**

If yes, please mark with an "X", the components that comprise the firewall design:

a. Authentication Server? ______

b. Screening Router? ______

c. Bastion Host? ______

d. Application Proxy Servers? ______

e. Other? __________________ ______

Please provide product and vendor name of the firewall device.

14. Where are the rules or restrictions documented for the firewalls, routers, bridges, and gateways? Please provide a copy.

15. Has a risk analysis been performed on this AIS within the last two years?

yes _____ no _____

16. How are system tapes or disks controlled?
Please explain - (physical control and operational procedures)?

B. NETWORKS

17. What services are provided? (FTP, RUSER, SYSTAT, Sendmail, AFTP, FINGER, TFTP, GOPHER, others?)

18. Are users provided information (Banner, HELP) about the system prior to a successful login?

yes _____ no _____

19. Is there a network monitor terminal for the on-line system?

yes _____ no _____

** 20. Are there test equipment, sniffers, or software being used to monitor the network?

yes _____ no _____ N/A _____

** 21. Is there remote access to this AIS?

yes _____ no _____

C. SOFTWARE

** 22. Describe the system and version levels and application(s) software used in the operation of the AIS.

Operating System:

Applications Software:

Security Software:

Network Software:

Freeware Software:

23. Is there a procedure established for receiving and implementing security and system updates for this AIS?

System **Security**

yes ______ no ______ **yes ______ no ______**

** 24. Does the site maintain a log of all system and security patches?

System Security

yes ______ no ______ yes ______ no ______

25. Is there any security software (i.e., SATAN, COPS, CRACK, etc.)

used to test the security vulnerabilities of this AIS?

yes _____ no _____

If yes, have the vulnerabilities been corrected?

yes _____ no _____

** 26. If software is used to restrict remote users, what approach is used (WINDOWS, captive accounts, file (rewrite) protection, etc.)? Please be specific.

27. Do all super users and System Administrators have a regular login account (non-privileged)?

yes _____ no _____

28. Is it possible to designate a file as readable, writeable, and executable? And is it possible to do this for the file owner, group and world?

possible? implemented? File owner _____
Group _____
yes _____ no _____ yes _____ no _____ World _____

29. Is there an automatic terminal logoff after x minutes of inactivity?

yes _____ no ______ x = _____

30. Is each modification to the operating system software accomplished by more than one knowledgeable individual?

yes _____ no _____ How many? x = _____

** 31. Does the system accept batch processing?

yes _____ no _____

D. USER IDs and PASSWORDS

32. Are one-time passwords or safe passwords used? A safe password is one that is difficult to guess.

yes _____ no _____

If safe passwords are used, how are they validated?

** 33. Provide answers for the following questions concerning passwords.

a. Are they unique for each user except
system operations personnel? (y/n) ______

b. Are they unique for each operator? (y/n) ______

c. Are Group Passwords used? (y/n) ______

d. Are System Passwords used? (y/n) ______

e. Are passwords changed periodically? (y/n) ______

f. What is the maximum change period? (y/n) ______

g. Is the change period software enforced? (y/n) ______

h. Are passwords automatically disabled
after the change period expires? (y/n) ______

i. How long after the change period? (y/n) ______

j. What is maximum password size? (no.) ______

k. What is minimum password size? (no.) ______

l. Are passwords assigned or user created?

Assigned ______ User Created ______

m. How many password histories are kept on disk? (no.) ______

n. How often are router passwords changed?
Indicate the applicable time interval with the amount.

Days ______ Months______ Years ______

Never ______ Passwords Not Used ______

o. Are System Administrator or super user passwords
handled differently from the above responses? (y/n) ______

If yes, please explain.

34. Provide the following information concerning users.

a. Number of individual IDs? ______

b. Number of user groups? ______

c. Number of vendor IDs? ______

d. Number of privileged (super user) IDs? ______

e. Number of System Administrator IDs? ______

f. Number of Security Administrator IDS? ______

g. Number of users with Auditor IDS? ______

h. Number of dial-in users? ______

i. Number of Guest or Public user IDs? ______

j. Are userIDs disabled after a pre-set number of failed logins? (y/n) ______

k. Number of login failures? (no.) ______

35. How are user IDs, passwords, and logins administered?

User IDs:

Passwords:

Logins:

** 36. Are vendor and maintenance user IDs and passwords disabled to prevent access after the following events?

EVENT	VENDOR		MAINTENANCE	
After a visit?	yes _____	no _____	yes _____	no _____
Installation of new software?	yes _____	no _____	yes _____	no _____
Upgrade of existing software?	yes _____	no _____	yes _____	no _____

** 37. Does the system lock out a user after a set number of unsuccessful log-in attempts?

yes _____ no _____ How many? x = _____

** 38. Is there a current access list of all personnel authorized to access the system, including access to remote devices?

yes _____ no _____ Approximate no. _____

** 39. What privileges do the operations personnel have?

40. Can the System Administrator login via a remote terminal?

yes _____ no _____

** 41. What is the procedure or process for adding a new user to the system?

42. What is the procedure or process for adding a system administrator or super user to the system?

E. AUDIT

** 43. Can the AIS produce an audit trail for security related events?

yes _____ no _____

** 44. What events can be audited on a daily basis and which are normally or always selected?

	Possible	Selected
system access (logins)?	_____	_____
failed login attempts?	_____	_____
break in attempts (x number of failed logins)?	_____	_____
unauthorized file access?	_____	_____
privileged (super user) users?	_____	_____
modifications to user authorization files ?	_____	_____
modifications to audit log?	_____	_____
access to system files?	_____	_____
dial-in modem traffic?	_____	_____
system operator activities?	_____	_____
file modifications?	_____	_____
other? (___________)	_____	_____

45. Are all security files (password tables, authorization tables, audit

logs, and audit reports) stored in protected format or encrypted?

yes _____ no _____

** 46. Are audit log files protected, once they are removed from the AIS?

yes _____ no _____

If yes, please explain how these files are protected once removed from the AIS.

** 47. What procedures are followed for security violations or suspected violations?

** 48. Does the security staff inform users of security incidents which involve the AIS?

yes _____ no _____

F. TRAINING

** 49. Is annual security training required for everyone with access to this AIS?

yes ______ no ______

** 50. What kind of special training do Security Administrators receive?

Appendix B. Nascom Access Control Policy Waiver Request

NASA FACILITY: SYSTEM NAME:

DATE: MAILING ADDRESS:

TECHNICAL CONTACT:

PHONE NUMBER:

DESCRIPTION OF VULNERABILITY (keyed to handbook or checklist):

WAIVER REQUESTED (Specific operational deviation):

TYPE (1,2,3):
1 = Temporary (**4** to 6 months)
2 = Long-Term (7 to 36 months)
3 = Permanent (over 36 months)

ESTIMATED RESOLUTION DATE:

JUSTIFICATION (use additional sheets, if necessary):

____
Signature of Requester

(To be filled out by Nascom and returned to requester)

Date received: WR NO. ____

Security Analyst:

Analyst's comments: __________________________

______ CONCUR __________________________
Nascom Automated Information
Security Officer (AISO)

______ APPROVED

Signature __________________________ Date: _______
Chief, NASA Comm. Div.

NOTE: Each deficiency is to be identified by a separate waiver request.

Appendix C. MODNET and NOLAN Security Policy

A copy of the MODNET and NOLAN Security Policy is provided in this appendix. The policy is taken from the MODNET and NOLAN User's Guide (Authority 1.6.h).

MODNET-NOLAN SECURITY POLICY

No dual-attached connections are permitted. Users must choose between connection to the Open or Closed segments. (Connection to the CNE is also an alternative.) All communications to the CNE and NSI from a MODNET-NOLAN host will be through the Nascom-provided single point of access. Nascom configured and controlled routers with filtering will be provided at all Internet connection points, providing minimal low-level security. Connection directly to the Internet at remote sites is allowed on the Open segment, with approval of the configuration by a Nascom security audit team. C2-level security is required for dual-connected remote hosts.

The Closed Segment provides a high level of security and limited access. No direct user Internet connectivity is permitted on the Closed Segment. The Closed Segment will be protected by the MODNET and NOLAN Secure Gateway, which provides filtering at the network level based on known IP source and destination addresses and IP services utilized. To communicate with the Closed Segment (i.e. FDF, CMF, TPOCC, etc.), users must log into an application firewall that supports IP services such as telnet, FTP, Mail, X-Windows, etc. External users, including Open Segment users, are required to use one-time passwords or encrypted passwords.

The Open Segment allows access to and from unknown sources on the Internet. Minimal filtering will be provided by the MODNET and NOLAN network. The users will provide security at the application level.

Remote users with Internet connectivity will be connected to the Open Segment, and must implement C2 security. The following Audit Events must be implemented, as a minimum:

- **file read**
- **file write**
- **file creation**
- **file deletion**
- **network events**
- **login_logout**
- **program execution.**

All new users who wish to be connected to MODNET and NOLAN must fill out the Network Connection Application. The Nascom Policy Statement will be distributed with the application. Projects and users will clearly state in the network connection application which segment, Open

vs. Closed, they will require connection to. Users on the Closed Segment will submit connectivity requirements for entry into the Secure Gateway Rulebase.

Nascom formalizes agreements with network users through Memoranda of Agreement (MOA). MOAs clearly define the connectivity requirements of the Projects and users as understood by the system personnel. The Project Managers will sign off on the MOAs. MOAs with the Project and users on the Closed Segment will include the detailed security filtering requirements to be entered in the Secure Gateway filtering Rulebase.

Code 540 operations personnel will provide security administrator functions for the secure connectivity of the MODNET and NOLAN to the CNE and Internet. The Security Administrator will monitor the logging, add and track new Project and user connection requirements to the Secure Gateway Rulebase, and report infiltration to the Nascom Security team.

Projects must obtain waivers for not adhering to the recommendations in this policy. Waivers are considered on a case-by-case basis, and will be documented by the Code 540 Automated Information Security Officer (AISO). Waivers affecting users on the Closed Segment will require their consent and approval.

Abbreviations and Acronyms

ACF2	**Access Control Facility 2**
AIS	Automated Information System
AISO	**Automated Information Security Officer**
CM	configuration management
CMF	**Control Management Facility**
CNE	**Center Network Environment**
CSR	communications service request
DCN	document change notice
DDCS	Data Distribution and Command System
DEC**net**	Digital Equipment Corporation network
DMS	Digital Matrix Switch
DOD	Department of Defense
EBnet	**EOSDIS Backbone (EB) network**
EOSDIS	**Earth Observing System Data and Information System**
FDF	Flight Dynamics Facility
FTP	**File Transfer Protocol**
GSFC	Goddard Space Flight Center
ID	identifier
IP	Internet Protocol
LAN	local area network
MAN	metropolitan area network
MDM	**Multiplexer/Demultiplexer**
MOA	**Memorandum of Agreement**
MO&DSD	GSFC Mission Operations and Data Systems Directorate
MODNET	MO&DSD Operational Development Network
MSFC	Marshall Space Flight Center
MSS	Message Switching System

NASA	National Aeronautics and Space Administration
Nascom	NASA Communications
NHB	NASA Handbook
NMI	NASA Management Instruction
NOLAN	Nascom Operational Local Area Network
NSI	NASA Science Internet
OSI	Open Systems Interconnection
PC	personal computer
PSCN	Program Support Communications Network
QA	quality assurance
RACF	remote-access control facility
SATAN	**Security Administration Tool for Analyzing Networks**
STD	standard
TCP	Transmission Control Protocol
TPOCC	**Transportable Payload Operations Center**
TTY	teletype
WAN	wide area network
XNS	Xerox Network Services

Glossary

Access

A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Access Control

The process of limiting access to the resources of a system only to authorized programs, processes, users, or other systems (in a network). Synonymous with controlled access and limited access. Restrictions controlling a subject's access to an object.

Audit Trail

A set of records that collectively provide documentary evidence of processing used to aid in tracing from the original transactions forward to related records and reports, and backwards from records and reports to their component source transactions.

Automated Information System

Any equipment or interconnected system or subsystem(s) of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes mainframe computers, minicomputers, workstations, word processors, automated office support systems, communications systems, networks, and their interconnecting hardware, and test equipment

Bridge

A bridge is a device that monitors data on each of the connected LANs and makes decisions about which data packets should be transferred across LANs and which should remain on the LAN where they were generated. Bridges connect LANs with compatible protocols at the Media Access Control sublayer of the Data Link layer in the OSI protocol model. Bridges can connect Ethernet-to-Starlan, Ethernet-to-Token Ring, etc. Because the connection is under the three layers that define LAN protocol [such as Transmission Control Protocol/Internet Protocol (TCP/IP), DECnet, or Xerox Network Services (XNS)], bridges are protocol-insensitive and transparent pipelines.

C2

A security level defined by the Trusted Computer System Evaluation Criteria (TCSEC) (DOD 5200.28-STD) (see SECURITY LEVEL)]. A C2 level commonly called "Controlled Access Protection" requires discretionary (i.e., author) control, object reuse rules, and auditing of security-relevant events.

Certification

The technical evaluation of a system's security features, made as part of and in support of the approval or accreditation process, that establishes the extent to which a particular computer system or network's design and implementation meet a set of specified security requirements.

CRACK

A password checking program which is used to determine if passwords, on a given system, are readily guessable.

Discretionary Access Control

A means of restricting access to objects based on the identity and need-to-know of the subjects or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing on that permission (perhaps indirectly) to any other subject (unless restrained by mandatory access control).

Firewall

A collection of components used to block or filter transmission of certain classes of traffic. There are three types of firewalls: packet filtering, circuit gateways, and application gateways.

Gateway

A hardware device that provides a communication path between two LANs using different LAN types and protocols. Gateways may perform protocol conversion for all seven layers of the Open Systems Interconnection (OSI) model and may be application-specific.

Local Area Network

The connection of AISs within a local area. LANs use a serialized bus with a cable length of up to several kilometers. LANs are local networks with relatively short ranges and are commonly used within a single building or floor.

Metropolitan Area Network

A computer network that connects several AISs within a metropolitan area. MANs are extensions of shared-access LANs (i.e., extended to the size of a city and its suburbs) and are designed to take advantage of the high speeds possible with fiber optics.

Object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it constrains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printer, and network nodes.

Password

A private character string used to authenticate an identity.

Process

A program in execution. A process is completely characterized by a single, current execution point (represented by the machine state) and address space.

Program Support Communications Network

The administrative network connecting the NASA centers with NASA Headquarters. This network is managed by Marshall Space Flight Center (MSFC).

Repeaters

Repeaters connect two similar LANs at the OSI physical layer or cable. Both media must be the same (i.e., a repeater can connect two Ethernets or two Token Rings, but not an Ethernet to a Token Ring). Repeaters simply repeat signals received on one LAN to the other.

Routers

Routers connect LANs with common protocols at the network layer and above. Because routers connect at the network layer, they are protocol-sensitive and thus can link two TCP/IP, DECnet, or XNS-based LANs, but not their combinations.

Security Architecture

The subset of computer architecture dealing with the security of the computer or network system.

Security Level

The combination of a hierarchical classification and a set of nonhierarchical categories that represent the sensitivity of information. The currently accepted method of determining the security level for NASA is NHB 2410.9. This handbook defines the various security or criticality levels and lists the generic protection requirements for each level.

Security Policy

The set of laws, rules, and practices that regulate how an AIS manages, protects, and distributes sensitive information.

Subject

An active entity (generally in the form of a person, process, or device) that causes information to flow among objects or changes the system state. Technically, a process and domain pair.

User

Person or process accessing an AIS either by direct connection (i.e., via terminals) or by indirect connection (i.e., via preparation of input data or receipt of output data that is not reviewed for content or classification by a responsible individual).

Waiver

A request for relief from meeting a security standard or practice until a satisfactory solution can be implemented to correct a known deficiency.

Wide Area Network

A network or interconnection of AISs over a large geographic area, such as between cities.

Distribution List

Organization	Name of Recipient	Copies
GSFC/540	Butler, T.	1
GSFC/540	Smith, S.	1
GSFC/540	Turner, V.	1
GSFC/540	Salzberg, I.	1
GSFC/540	Kirwan, E.	1
GSFC/541	Torain, B.	1
GSFC/541	Smith, J.	1
GSFC/541	Steedman, J.	1
GSFC/541	Garman, C.	1
GSFC/541	Douglas, S.	1
GSFC/541	Kirichok, M.	1
GSFC/541	Johnson, M.	1
GSFC/541	Suprock, C.	1
GSFC/542	Hill, P.	1
GSFC/542	Fath, B.	1
GSFC/542	Lawless, E.	1
GSFC/542	Norman, S.	1
GSFC/542	Richter, M.	1
GSFC/542	Zgonc, G.	1
GSFC/542	Duffy, D.	1
		20
AlliedSignal Technical Services Corp. (ATSC)		
ATSC/Nascom	Nascom CM Library	1
SEAS/540	Lee, R.	1
		2